METHOD AND APPARATUS FOR SECURE DATA TRANSMISSION SYSTEM

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to data transmission systems and, more particularly, a method and apparatus for transmitting a secure document so that a recipient can review the document and provide a secure response without special apparatus at the receiving end.

2. Description of the Related Art

Most secure data systems of the prior art have required special equipment at both the transmission and reception ends in order to recover the secure information and provide a secure reply. Such systems usually include encryption and decryption devices at both ends of a message.

Clearly, the sender must have apparatus for converting plain text into some encrypted or encoded format that is illegible to anyone lacking compatible apparatus at the receiving end. With so many different types and styles of encryption and encoding in an attempt to achieve secure communications, and in the absence of a single, standard system, the probability is low that the sender and receiver will have compatible encryption systems.

The Internet (global computer network) is a fast growing medium for information exchange. Although much of this information is of dubious value, the usefulness of the Internet as a vehicle for electronic commerce means that there is an increasing need to provide security for data transmissions.

Different types of data transmissions present different risks and obstacles and require suitable protection from tampering, corruption, theft, unauthorized access, etc. Many software and hardware products that provide such security for Internet data require that users at both ends of the transaction (i.e. sender and receiver) have the same software components or at least a highly compatible set.

This requirement for having nearly identical software at both ends of a data exchange is highly limiting. Imagine an exchange that involves parties from five different organizations! This requirement can be (and has been) dealt with by products such as Norton Secret Stuff from Symantec, Zip and WinZip from PKWare, Universal Envelope from VIAexpress, and Envelope98 from the assignee of the present invention. Each product "wraps" the message to be transmitted in an "electronic envelope". This "envelope" contains all the computer code and logic necessary to protect the message during transmission and to extract it at the receiving end.

Such an "envelope" can successfully protect data sent to a receiver.

However, in many cases the receiver may want (or be required) to reply and the reply must also be protected during transmission. Here again, a problem reoccurs. The receiver is required to install and use some type of cryptographic software or hardware to protect the reply.

Most importantly, this problem must be solved in a way that is simple to use and doesn't require an excessive amount of preparation (i.e. creating and distributing certificates and public keys, maintaining a authentication chain and a public key ring). Generally, in each case where it is necessary to transmit data securely and bidirectionally between two entities (either directly or through a private or public communication system) identical or highly compatible software and/or hardware must be installed at both ends. This presents difficulties whenever a party wishes to exchange information with more than one other party. Even then, it may be difficult to assure that both parties have equipment capable of communicating with each other.

Many products and technologies exist that can solve the problem. These include technologies known as PGP ("pretty good privacy"), PEM, S/MIME and SSL. In each case the systems are not cross-compatible (i.e. a message encrypted using the PGP system cannot by decrypted using S/MIME and vice versa). In addition, users of these systems are forced into a complicated series of operations to prepare for a data exchange (i.e. key generation, authenticity certification, etc.). Several systems require the participation of a trusted third party to authenticate the identity of the parties participating in the data transfer.

Although the existing systems are useful in certain situations, their acceptance has been slow and limited due to the high costs (in the form of computer resources and user time) and limited cross-compatibility.

For example, if two users from the same organization wish to communicate using PGP, they would exchange public keys using a central computer (authentication/key server). Such a server would, in essence, guarantee to each user the identity of the other as well as providing to each the other's encryption keys. Because most organizations would select a single system to use for secure information exchange (i.e. PGP), the users could now exchange e-mail easily and securely.

If however, the two users are from different organizations, there may be no central computer to use as a "certification authority". The users would then have to exchange keys in person or by mail. They could also rely on a trusted third party to provide this service. The two users would still have to establish a common standard with which to encrypt their data: PGP, PEM, S/MIME, etc. One or both might have to switch to this agreed upon

standard.

It quickly becomes obvious that the overhead created during this process greatly complicates the needed exchanges. If the exchange is between more than two users belonging to more than two organizations, the level of complexity increases rapidly. A simpler solution is required.

Two users, both with "electronic envelope" software, could exchange information without first agreeing on a standard system. However, each would have to install into their computer some form of electronic envelope system. Even the "electronic envelope" systems described above suffer from an inability to transmit data bidirectionally between parties except when all "transmitting" parties have installed the same cryptographic software onto their computers.

SUMMARY OF THE INVENTION

According to the present invention, there is provided to the user, the ability to send an "electronic envelope" across private and public communication networks including the use of e-mail. The sent information is protected from unauthorized access, corruption, tampering and theft while in transit and the "electronic envelope" allows the receiving user to decrypt the message without having to install any cryptographic software or hardware.

The invention includes a "secure reply" feature that allows the recipient of an encoded message to encrypt and return a message to the sender, again without having installed any cryptographic software. The present invention gives the receiver's reply the same level of protection and security that original encryption afforded the sender.

The present invention is also easier to use, only requiring the two participants to exchange keys (known as "passphrases") by any of the available modes of communication, such as a telephone conversation, postal mail, in person communication, or any other mode. Keys can be changed regularly, thereby enhancing security.

Not all users in an information exchange are required to install the systems of the present invention. For example, in a system where a service vendor was sending invoices (via e-mail) to selected customers, those customers would not need to install any cryptographic software. The present invention would provide all the necessary functionality to allow the secure return of payment instructions to the vendor. The same system using S/MIME or any of the other, prior art systems, would require all users to exchange keys with the vendor and obtain compatible software.

Imagine two people from different companies who need to communicate

securely, for example, Alice, who works for Widget Manufacturing Corporation (WMC), and Bob, an employee of WidgetBits, Inc., a supplier of components needed in the manufacture of widgets. Alice needs a proposal from Bob to supply WMC with widget components over the next 6 months.

Since the market for widgets is such a competitive environment, both Alice and Bob are keenly aware of the potential damage to their respective businesses should their competitors gain access to the information contained either in Alice's request or Bob's reply. Accordingly, they could use the system of the present invention to conduct their business.

Alice starts by creating a "request for proposal" (RFP) document using any word processor. She then uses the present invention to encrypt her document which "wraps" it in a self-decrypting "envelope". She also enables a feature to give Bob the ability to encrypt his reply. Lastly, she transmits this "envelope" to Bob using any means she chooses - e-mail, file transport, or copying the file to disk and mailing it, to name a few.

To continue with the "envelope" analogy, when Bob receives the encrypted message, ("envelope") he opens it using the previously received "passphrase". The document is then decrypted. Bob is assured that no one has seen the document while it was in transit and that is was not corrupted or modified in any way.

Bob is now free to write his proposal. Again, using any word processor, he creates a document to send to Alice as his reply. When the document is ready, he once again opens the original "envelope" and supplies the passphrase. The option to create a secure reply is offered. If selected, the proposal is encrypted using the same passphrase that allowed decryption of the original message. Bob is then free to transmit his proposal back to Alice as a secure reply file using any means at his disposal.

Upon receiving the secure reply, Alice decrypts it using the original encryption-decryption program of the present invention together with the original passphrase. She can now read Bob's proposal and continue to conduct her business.

Another example in which the present invention can be used is an implementation of a billing and payment processing system employed in an Electronic Commerce environment. A system of this type would use the ability to provide a secure reply for a more specialized purpose and so would implement a different user interface than in the preferred embodiments of the present invention. Nevertheless, the ability to provide a secure reply is unchanged.

In a (very simplified) electronic billing and payment system, the two

parties correspond via an e-mail connection. Both parties would first agree to a pass word or phrase (which may also be a Personal Identification Number or "PIN") with which the data being transferred is cryptographically secured. The vendor sends the customer an invoice or statement reflecting customer activity and an amount due. The customer responds with payment instructions and an authorization.

For example, the vendor would prepare a statement. This statement would then be encrypted and enclosed in an "envelope" along with a special purpose program designed to gather the customer's payment instructions. This envelope is transmitted through e-mail to the customer. The customer opens the envelope using the pass word or phrase established by prior agreement with the vendor. Once the contents of the envelope are decrypted, the statement is presented to the customer.

When the customer is ready to make a payment to the vendor, the envelope is again opened and the special purpose program automatically executes, presenting the customer with various payment options. When the customer has selected a payment method, a secure reply is generated (the payment selection program having automatically requested a secure reply from the original envelope).

The secure reply is then e-mailed back to the vendor. When the vendor receives the customer's secure reply, an automated process decrypts the reply, extracts the customer's payment instructions and submits them for further processing. A working implementation of this electronic billing and payment system exists in proprietary products of the assignee of the present invention.

The purpose of providing a secure reply feature is to allow two computer users to communicate securely (i.e. using encrypted data files) in circumstances where only one of them has the cryptographic software needed. Whatever software is needed to both decrypt the sent message as well as encrypt the reply is transmitted with the original message.

A secure reply may also be used in any circumstance where all that is needed is an acknowledgment that the message has been received and correctly decrypted since a secure reply cannot be created without knowledge of the correct pass word or phrase. In addition, it may be that the contents of the acknowledgment itself may be useful to a rival business or individual and so the encrypted reply provides the necessary security.

A working implementation of this electronic billing and payment system exists in proprietary products of the assignee of the present invention. The purpose of providing a secure reply feature is to allow two computer users to

communicate securely (i.e. using encrypted data files) in circumstances where only one of them has the cryptographic software needed. Whatever software is needed to both decrypt the sent message as well as encrypt the reply is transmitted with the original message.

For a different example, in an increasingly complex world it often become necessary for experts in diverse fields or specialties to work together in confidence. Many times these people must cooperate with little or no advanced notice and the information to be exchanged is of a sensitive or secret nature. All parties would like to execute an information exchange with a minimum of overhead expenditure.

Imagine, for example, a law firm (XYZ Partners) represents a well known party in contentious litigation. All the materials pertaining to this case are considered highly sensitive. Nevertheless, XYZ needs to consult with lawyers at another, distantly located firm (HIJ) specializing in an one area of the case. Time is, of course, of the essence.

Using the present invention, lawyers at XYZ can send documents to HIJ securely through the public e-mail network. The lawyers at HIJ can then edit any document sent or add their own input to the document and, using the present invention, reply to XYZ with the same level of security.

All parties are protected by the secure transmission and the collaborative effort requires a minimum of overhead and preparation.

Accordingly, it is an object of the present invention to provide a method and apparatus to send an encrypted message which permits an encrypted acknowledgment that a secure document had been successfully received and decrypted without special hardware or software at the site of the recipient.

It is an additional object to retrieve a secure document from a remote computer user by first sending an encrypted transmission with a dummy file.

It is a yet another object to foster a secure cooperative work environment by allowing two computer users to cooperatively develop a document such as a proposal, business plan, computer software, mechanical schematic, or the like. The document would be sent from the first user to the second using an protected transmission and the second user could then make any needed modifications to the document and return it using the present invention.

Yet another object of the invention is to enable the secure distribution of software with user registration information being returned using the present invention.

A further object of the invention is to permit the distribution of information about a product under development to a restricted group of computer users. Those users could respond with comments, suggestions, etc.

in accordance with the present invention.

The novel features which are characteristic of the invention, both as to structure and method of operation thereof, together with further objects and advantages thereof, will be understood from the following description, considered in connection with the accompanying drawings, in which the preferred embodiment of the invention is illustrated by way of example. It is to be expressly understood, however, that the drawings are for the purpose of illustration and description only, and they are not intended as a definition of the limits of the invention.

BRIEF DESCRIPTION OF THE DRAWING

FIG. 1 is flow diagram showing the principles of operation of the present invention.

FIG. 2, including FIGS. 2a-2d, inclusive are flow charts of the steps taken in implementing the sending, receipt and return of secure information;

FIG. 3, including FIGS. 3a - 3d, inclusive is a more detailed flow chart of the process of the present invention; and

FIG. 4 including FIGS. 4a - 4b is a flow chart of an embodiment of the present invention for secure billing and payment transactions,

DESCRIPTION OF THE PREFERRED EMBODIMENTS

The following Program Flow descriptions and diagrams describe the present invention as currently implemented by the assignee in a product offered by the applicant under the trademark Envelope98™ which is a secure transmission product. The same procedures apply in other situations with slight changes to the user interface.

Starting with FIG. 1, there is shown a generalized overview illustrating the present invention in use. Utilizing a specialized program, a message (envelope.exe) which includes an executable program and encrypted files is created which, when received and executed, decrypts the information contents upon the presentation of a preselected pass word or phrase. The entire message can be sent to a receiver using e-mail, a modem to modem file transfer over telephone lines, or may be recorded upon a disk which can be sent by courier or through the mails.

At the receiving end, the receiving party executes the program (envelope.exe) that is an integral part of the message. The receiving computer then asks for the agreed upon pass word or phrase and, upon its provision, operates upon the encrypted files to decrypt them. The message is then

given the option to provide a secure encrypted reply.

If the option is selected, after a reply is prepared, the received message is executed again and the reply option, when invoked, encrypts the reply message and the reply can be transmitted back to the originator using any of the same methods that could be employed in sending the initial message. Once the originator receives the message, his equipment permits a decryption of the returned file.

As shown in FIG. 1, the initial step is the creation of the envelope.exe file 12, which is explained in greater detail in connection with FIG. 2, below. In FIG. 1, the global computer network is used to transmit the file 12 in the transmitting step 14. At the recipient's end, the file is received 16 and the transmitted program is executed 18. If the recipient desires to proved an encrypted reply, the received program enables the preparation of the reply 20 and this reply is returned 22 through the global computer network. The reply is received by the original sender 24 who possesses the program to decrypt the reply 26.

In FIG. 2a, a preferred embodiment of the present invention is detailed, explaining the layout of the message which is to be transmitted. Initially, the user determines which files are to be transmitted, the encryption algorithm and pass word or phrase, whether to include the secure reply option, any other user-specified information and a name for the file. In the next step, the decrypt engine code is written and is attached to the other file elements.

Each file that is to be transmitted is sequentially retrieved and, if the option is selected, compressed. Next, special data is computed and in a successive step is encrypted using an algorithm that is user determined. A file header is prepared and the file is set for transmission.

Each of the remaining selected data files, is, in turn, processed through the same steps until all selected files have been compressed (if the option has been selected) provided with error detection codes, file size information and any other information which must be added and encrypted.. After all of the files are processed, the message is closed and is ready for transmission by any available means including the global computer network, modem to modem direct transmission, or storing on transportable media and forwarded by mail or courier.

With reference now to FIG. 2b, the steps performed at the receiving end are outlined. When the transmitted program is executed (envelope.exe), the envelope header is read and the information relative to the number of files transmitted is noted.

The various user instructions are then acted upon including the designation of the files to be extracted, the destination on the recipient's computer, pass word or phrase, the files, if any, to be included in a reply and, if a reply is to be made, the destination of the reply.

Next, each of the transmitted files is, in turn, decrypted, decompressed, is verified through an integrity check and written to the preselected destination in the recipient's system. If a secure reply is to be made, the next steps are to be found in FIG. 2c.

After the message is received and if the receiving party is ready to send a reply, the user again executes the received program (i.e. runs the envelope.exe instruction). The program is aware (through the use of a flag in the message header) that the original contents have already been decrypted and asks the user if a secure reply is to be created.

If the user requests a reply, the program asks for the name of the file or files to encrypt and, after encrypting the files, "wraps" them in a reply header. Notice that no decryption program is returned with the reply as it is a precondition of creating the message that the software needed to decrypt the reply is present.

If the secure reply option was provided and elected, the user determines which files to send, a file name, a password or pass phrase and a header. The received program, when executed again compresses (if desired) each file that is to be returned, special information is collected and each file is encrypted by the program which was transmitted to the recipient, who has no other encryption or decryption software available to his system. When all the files to be returned have been processed, the file is closed and the reply message is returned.

The steps to be followed when the reply is received at the original sender's location are indicated in FIG. 2d. The original sender's program can read the header of the reply and extract all of the necessary processing information. The original recipient's reply instructions are then processed which include the files to be extracted, the pass word or phrase and the destination of the transmitted files.

In turn, each returned file is decrypted using the appropriate algorithm. The file is next decompressed, if necessary. The contents are checked for integrity and the file is stored in the selected destination. When all files have been stored, the program is deemed complete.

Turning to FIG. 3a, the process at the receiving end is illustrated in a branching flow diagram. At the start, there is a choice of having a reply option on the command line. If no file name is present, a flag is set

indicating that a reply is to be created and a file name is generated. The program will then ask for the previously agreed upon pass word or phrase. Once provided, a crypt key is generated from the pass word or phrase and the message can be opened and read. After the header is read, the program checks to see if the reply option is indicated by a set flag but the message has not yet been decrypted. If so, a warning is given and the option to continue is offered. If the choice is not to continue, the program is exited.

Referring to FIG 3b, if the process is to continue, the next branch point is if the flag is not set but the message has been decrypted. If affirmative, the user is requested to decide if a reply is desired. If no reply is desired, the flag is cleared. If a reply is desired, the flag is set.

The next branch point examines the flag. If it is set, the key is verified, If not, the message is decrypted and the program is exited. The key is verified and if correct, the next check is made. If the key is not correct, the program exits. The next step is to check the reply file name. If one is not yet set, a name is acquired from the user. If there is a name set, a check is made to see if the file is accessible.

The process continues with reference now to FIG. 3c. A name is created for the reply output file. The user is asked if the created name is acceptable. If not, an acceptable file name is acquired. If so, it must be determined whether the file can be created. If not, the program is exited. If it can, the file is encrypted, a header is written for the "envelope" and the datafile and a message is displayed that the process has been completed.

Turning now to FIG. 3d, the process at the original message source is not reviewed with the receipt of the reply message. Because the original operating program is at this source, the reply can be immediately opened and read. The header identification is noted and the pass word or phrase is supplied. The crypt key is created from the pass word or phrase and the file name for the decrypted output file is supplied. If the key being used is incorrect, the program is exited. If correct, the datafile is decrypted and verified as being correct and uncorrupted. If it is not, an error message is displayed and the program is exited. If it is correct, then the program is exited without the error message.

An alternative embodiment of the present invention is illustrated in the flow diagram of FIG. 4 which includes FIGS. 4a and 4b. In this embodiment, a simplified program is illustrated for secure billing and payment. The bill is presented to the software program which compresses the bill, encrypts it and creates a secure "envelope". A e-mail message is created

which includes the encrypted bill. The e-mail server then sends the bill through the global computer network, sometimes calles the Internet,

Turning now to FIG. 4b, the message including the bill is received and the attachment is opened. A browser is launched which fetches, using the global computer network, a decryption program from a web site server specially authorized to perform this service. Once obtained, the decryption program is run.

The recipient is prompted for a Personal Identification Number ("PIN") or pass word or pass phrase. The PIN is checked for validity. If invalid, it is printed out and the program is shut down. If valid, the program then decrypts the message and sends a confirmation over the global network to the sender. The bill is then displayed in the browser window and a connection is arranged to a billing website. At this point, a payment authorization can be sent or the billing website can furnish other bill paying options. The biller website can be a neutral service provider or a financial institution which can be authorized to pay all or a portion of the bill or otherwise meet the payment responsibility.

Thus there has been described a system in which secure messages can be transmitted and secure replies can be created by the recipient without the need for any special software programs installed at the recipient's computer. The secure message includes a program, which when executed, enables a viewing of the received message and the preparation of a secure reply. However, the recipient cannot use the program to create new, secure messages to third parties or to permit those third parties to create secure replies.

The system of the present invention lends itself to the secure exchange of data or for secure financial transactions in which bills can be presented and paid. In one embodiment, any means of communication may be employed including, but not limited to the delivery of portable media. In an alternative embodiment, the transmitted program can be abbreviated so that a link is created through the global computer network that supplies the software necessary to decrypt the message and create the secure reply. Further a separate link can be created with a secure financial services site that can handle a financial transaction based on the submission of a secure billing.

The scope of the invention should be limited only by the scope of the claims attached below.